UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

JAVIER LUIS,

Plaintiff,

vs.

JOSEPH ZANG, et al.,

Defendants.

Civil Action No. 1:12-cv-00629

Dlott, J.
Bowman, M.J.

PLAINTIFF'S FIRST MOTION FOR LEAVE TO FILE SECOND OBJECTION TO REPORT AND RECOMMENDATION (DOC.# 225)

Plaintiff, Javier Luis, herein submits his first motion for leave to file his Second objection to the Magistrate's Report and recommendation (Doc. # 225) Pursuant to Rule 72 of the Federal Rules of Civil Procedure, objection to the Magistrate's report and recommendation ("RR") (Doc. # 225) for the reasons stated in the attached memorandum in support. It should be noted that Plaintiff had some problems filing his objection on Friday, including a strange error that had him file the objection an objection as well as a motion for judgment on partial findings.[1] This submission should be seen to supersede and/or supplement the previous one.

[1] For some reason the system would not allow submission as usual, blocking me and making me re-sign in multiple times. When I finally got back to the submission page, apparently multiple filing options were entered. Plaintiff would like to withdraw that particular filing, although he assumes the properly filed document was accepted.

Dated: May 7, 2018

Respectfully Submitted,

/s/ Javier Luis
JDLuis65Ohio@gmail.com

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Motion was filed electronically on May 7, 2018. Parties may access this document through that system.

/s/ Javier Luis, Pro Se

MEMORANDUM OF LAW

Plaintiff objects to all of the MC's rulings in the RR, believing the reasoning used is flawed *ab ovo usque ad malain* – or at least in all of the following ways; (1) the RR wrongly opposes congressional intent in its construing of the Wiretap Act, and (2) the RR runs afoul of technical realities related to computer hardware and the delivery mechanisms running the internet, and (3) The RR runs counter to more recent and more technically sand constitutionally sound judicial interpretations of what comprises an "intercept." Perhaps most unfortunate of all, the RR is also (4) dangerously counter to our already battered privacy interests in this ever-changing Digital Age.[1]

Introduction

A few years ago, and much to its credit, the Magistrate Court (or "MC") impressively rejected decades of improper reasoning as to a critical issue within the Wiretap Act, while suggesting that "a rethinking of the definition of the 'contemporaneous' standard of intercept might be necessary and that the timing of the intercepted data's transmission should be irrelevant, allowing the ECPA to be applied." Gariella E. Bensur, *Cover your Webcam: e ECPA's Lack of Protection against Software That Could Be Watching You*, 100 Cornell L. Rev. 1191 (2015)[2].

[1] This issue has been argued many times in the five years the case has been in this forum. Although plaintiff again incorporates those arguments by reference, it is perhaps wise to also *directly* reference and re-argued those points herein. As such, many of these arguments will cite to plaintiff's own previously submitted documents containing those arguments–both in this forum and in his prior appeal.

[2] referring to *Luis v. Zang*, No. 1:11-cv-884, 2013 WL 811816 at *6–7 (S.D. Ohio Mar. 5, 2013). Available at: http://scholarship.law.cornell.edu/clr/vol100/iss5/4

Apparently something has since changed. Fast forward almost a half a dozen years, and now we find this same Magistrate Court recommending that this Circuit be guided by a dangerous and regressively narrow interpretation of the recently adopted "contemporaneous" standard of intercept; an old and never technically correct interpretation as to what comprises an "intercept" under the Wiretap Act ("the Act" or "ECPA"). Moreover, the Magistrate Court ("MC") has sided with circuits that have (plaintiff believes) improperly removed transient storage necessary to the transmission of data from the communications the Wiretap Act was meant to protect. No matter, whether it likes it or not, the Magistrate Court got it right the first time around and so the District Court should now wisely reject the recent RR in its entirety.[3]

Background

Although the Act/ ECPA's anti-interception provision does not in any way stipulate that "interception" of electronic communications must be contemporaneous with their transmission, subsequent circuit court case law, such as *Fraser v. Nationwide Mutual Insurance Co*. (352 F.3d 107, 113 [3rd Cir. 2003]), "has held that an 'intercept' under the ECPA must occur contemporaneously with transmission." However, other circuits have taken a more advanced approach, having either formally or informally adopted a broader approach to the intercept

[3] While nothing in this objection will change a thing in the lower forum, rights must be preserved on appeal and thus the submission of this lengthy document. Much of this objection has been copied and pasted from previous submissions that went fully unacknowledged and un-responded to by either of the courts in the the lower forum in the five years the case has remained here. Since nothing has truly changed in this case from the time those documents were submitted many years ago, it would seem proper and more efficient that Plaintiff simply incorporate those documents here by reference and incorporate those arguments herein. However, as evidenced in the MC's recent Order, many courts apparently disfavor such wide-scale use of argument incorporation. Nonetheless Plaintiff incorporates all relevant arguments made during this case. Most of those are located within six particular documents in the lower forum (Doc.#'s 91, 97, 118 and 222 in the 629 case and Doc. #'s 101 and 175 in the 884 case) and those argued in appeals. While all the earlier arguments are adopted by reference herein, they will be re-argued here again as a precaution. Any relevant arguments mistakenly omitted should nonetheless be considered already argued and properly objected to for appeals.

question that plaintiff believes is much more technically sound and constitutionally proper. In most of those cases the courts did not necessarily deviate or reject the standard recently adopted contemporaneous standard in this circuit – rather they simply recognized the full set and type of data meant to be protected by the Wiretap Act. In truth, a vast re-thinking of the contemporaneous standard –if not its rejection entirely– really *should be* explored in this case in order to right the many wrongs created by the judicial system in its decades long "emasculation" of the Wiretap Act.[4] Nonetheless, in the alternative, a mere adjustment or tweak of the terms is all that is necessitated for now to get this case its proper day in court; a necessary and critical adjustment that will also protect hundreds of thousands of future victims (mostly female) whose ongoing abuse by their spouses is exponentially increased buy their spouses use of this maliciously designed and marketed spyware. In fact, aiding the already battered and abused was the original reason Plaintiff brought about this lawsuit in the first place back in 2011.

From the start and throughout this case, Plaintiff has consistently argued against adoption of the narrow interpretation of the "contemporaneous" requirement of intercept, believing it has dangerously compromised the protection of our digital communications.[5] Plaintiff has previously advocated a case that more accurately dealt with the kind of advanced software used by most corporate peddlers of personal/employee monitoring spyware which affects hundreds of millions of employees and private citizens everyday.[6]

---

[4] As just one example, in *Potter v. Havlicek*, 2007 U.S. Dist. LEXIS 19 10677 *11, Judge Rose opposed "a hyper-technical application of the contemporaneous requirement emasculating the ECPA."

[5] *See ex.*, Doc #: 91 in the 629 case, at * 6, filed on 10/12/12; *Luis v. Awareness*, Case: 14-3601 Doc. # 26 at *7

[6] That case, *Klumb v. Goan* was decided within this Circuit, and Plaintiff still believes the approach should be mimicked by this District Court as it likely represents the wave of the future in such cases. In *Klumb*, a man sued his ex-wife under the Federal Wiretap Act, 18 U.S.C. § 2520(b), and the Tennessee Wiretap Act, Tenn Code. Ann. § 39-13-603(a). At trial, defendant argued that no intercept had occurred because the software used, a keylogger identical to WebWatcher named eBlaster, did not "intercept" the communications as that term has been previously defined in the Wiretap Act. However, the court applied a "router switching analysis" finding that "a wiretap occurs when spyware automatically routes a copy of an email, which is sent through the internet, back through the internet to a

Regardless, the Sixth Circuit decided to adopt the dangerously narrow contemporaneous standard – ironically while reversing this Court's prior decision to terminate this case. Nonetheless, there remains critical wiggle room even within that disastrous standard if it must be observed. Nonetheless, if upheld as is, the MC's ruling will reward and encourage continued and expanded abuses of the multiple loopholes in the ECPA that have been noted and criticized since the advent of the Internet and advanced spyware in the mid to late 1990's. In order to prevent being on the wrong side of history in this important arena of privacy, Plaintiff believes this Court should do the following[7]; 1) reject the RR while adopting a broader approach to what comprises an "intercept" under the Wiretap Act – one more in line with that evidenced by the 1st and 7th circuits (as well as similar rulings in various district courts) and , 2) rule that the definition of "intercept" should also include any acquisitions while instant messages, digital communications of any kind, and e-mails are in temporary storage , and 3) rule that this Plaintiff has standing because a competent jury could find from the evidence already submitted (by both parties as well as those in the previously connected case) that Plaintiff's case meets those requirements as ruled in those circuits. Plaintiff's more specific objections are listed below.

I. The Magistrate Court erred throughout the RR

As well explored in Plaintiff's objection to Magistrate's Order (doc #: 224) - whose arguments are incorporated herein as if written anew - the MC abused discretion and erred by refusing to consider amended reply that did point out specific facts in evidence that present

third party's email address when the intended recipient opens the email for the first time." The court found "ample evidence" to show that a wiretap had occurred. *Klumb v. Goan* 100836 (E.D. Tenn. 2012).

[7] Ideally, the District Court will adopt or at least advocate a different standard altogether – the more advanced, constitutionally and technically sound "router switching" analysis used by the Court in *Klumb v. Goan*, 2012 U.S. Dist. LEXIS 100836 (E.D. Tenn. 2012). Nonetheless, Plaintiff realizes such a request is likely just another "bridge too far" for this Court at this point.

issues at trial. Nonetheless, even without acceptance of the amendments, there is plenty of evidence in the Record that Awareness intercepted, disclosed, and intentionally used Plaintiffs Electronic Communications. This came in the form of Techs own submissions to plaintiff in discovery as well as that admitted into evidence. Significantly, acquisition of AP's communications was never even *challenged* by Tech as there was plenty of evidence available to prove it had done so. Thus, arguing arguendo, even if *somehow* Tech was properly found innocent of liability for the *intercepts*,[8] Tech's "use" and "disclosure" clearly violated the Act because Tech did not challenge or address AP's claims (in the lower proceedings or in appeals concerning the following; 1) its advertising for illegal use was illegal, and 2) that they *knew or should have known* the illegal nature of the intercepts it was acquiring, using and disclosing. Therefore, Tech's summaries and deliveries given its undisputed ability (and/or duty) to know the illegal nature of the intercepts is a clear violation of 18 U.S.C §§2511(1)(c), (d). Moreover, the MC erred by finding that a reasonable jury could not find that the intrusion into Plaintiff's privacy was wrongful.

II. Definition Of "In Flight" Not Clear And Volatile Memory Was Also Meant To Be Protected By The Act Which Prohibits Both The Interception Of Electronic Communications In Transit As Well As Those In Storage.

A. The Wiretap Act's plain language makes no distinction between electronic communications in transit and those in electronic storage.

[8] An Intercept (§2511) was found to have occurred, and it had to have been Tech itself that was found to have intercepted and it did acquire AP's communications on its personal servers. That violation alone, with or without liability later attaching, would have been enough for the purposes of enabling standing to sue under §2512, as it was a violation of §2511. Most courts recognize a cause of action for §2512 when in the presence of any violations of §2511.

Nowhere in the Federal Wiretap Act does it state that an electronic communication cannot be intercepted while it is in storage. In fact, the Wiretap Act never mentions "electronic storage" in any of its relevant provisions. Defendants would have this Court believe that the Act creates a dichotomy between electronic communications in transit and electronic communications in storage and that the Act only protects the former from interception. This is plainly untrue. The Act treats electronic communications in transit and in storage identically.

B. The plain language of the Wiretap Act does not require a contemporaneous requirement and Congress defines intercept to include acquisitions, which need not be contemporaneous under any standard.

The plain language of the Wiretap Act never states that electronic communications can only be intercepted simultaneously with their transmission. The Act applies to "wire communications," "oral communications," and "electronic communications"; each of these three communications are treated differently under the Act. 18 USC § 2511(1)(a) (LEXIS 2015). The Act's own language limits wire communications and oral communications to contemporaneous interceptions, but refuses to extend such an interpretation to electronic communications.

Until recently, this Circuit had yet to rule on the contemporaneous requirement of intercept. However, in an appeal of this case, the Sixth Circuit did adopt that long problematic requirement, stating "We therefore hold that, in order for an 'intercept' to occur for purposes of the Wiretap Act, the electronic communication at issue must be acquired contemporaneously with the transmission of that communication." *Luis v. Zang,* 833 F. 3d 619, 627 (6th Cir. 2016).

Therefore, for better or worse, the contemporaneous requirement is for now the accepted standard within this Circuit.

What matters most now is whether this Circuit will adopt the (plaintiff argues) outdated and "always technically wrong" narrow interpretation of that already overly narrow standard as adopted by the 3rd, 5th, 11th circuits, or whether it will adopt the various broader approaches embraced by many state wiretap acts, some district courts within this same circuit, and sometimes evidenced within the appeals courts within the 1st, 7th, and 9th circuits[9]; holistic legal approaches which plaintiff believes are much more enlightened as well as being constitutionally sound and technically proper. The differences between the circuits are critical distinctions that can help mold our digital privacy protections for many years to come. While the District Court is perhaps not a forum that can by itself change the operating standard, it could nonetheless take this opportunity to re-examine the plethora of outdated circuit decisions that the 3rd, 5th, and 11th have used as the foundation for their contemporaneous arguments; one that requires a different treatment of electronic communications/emails in storage than those in transit. As previously discussed, that distinction is not supported by the Act nor is it found within its plain language. Congress never excluded electronically stored information from electronic communications, but it did from wire and oral communications.

By the Act's plain language, canons of construction, and the legislative history of the Act, it is obvious that Congress did not intend for electronic communications in storage to fall beyond the purview of the Act, and that to do so would produce an absurd result in the

[9] as far as plaintiff knows, the 1st, 7th, and 9th have also adopted a similar standard however their approaches have been broader and more technically sound than the other circuits, in plaintiffs opinion. Their reasoning evidences a more proper and constitutionally sound approach and this Court should mimic their better findings.

interpretation of the Acts protections. Such an approach is supported by the reasoning used in *Councilman*, as follows.

> The district court seemed to agree with one predicate of the Government's argument when it acknowledged that "technology has, to some extent, overtaken language" and that "[t]raveling the Internet, electronic communications are often—perhaps constantly both `in transit' and `in storage' simultaneously." *Councilman*, 245 F. Supp. 2d at 321. This apt observation should have prompted a different legal conclusion.
>
> All digital transmissions must be stored in RAM or on hard drives while they are being processed by computers during transmission. Every computer that forwards the packets that comprise an e-mail message must store those packets in memory while it reads their addresses… Since this type of storage is a fundamental part of the transmission process, attempting to separate all storage from transmission makes no sense.

This Court should find the more recent string of cases that apply the Act to electronic communications in storage more persuasive than those of the outdated cases relied upon by the circuits that adopted the narrower interpretation; cases that rely on a version of the Act that has since been amended.

III. The MC Ignored The Unique Qualities Of Webwatcher Then Applied Cases Featuring Outdated And Totally Different Types Of Software Within Her Reasoning.

A. The MC Ignored fact that WebWatcher is a type of automatic routing software that employs *continuous surveillance*

As properly explored in Councilman, the use of automatic routing software is a game changer when deciding whether or not an "intercept" occurred under the Wiretap Act.

> [U]nder the narrow reading of the Wiretap Act we adopt ., very few seizures of electronic communications from computers will constitute 'interceptions.' . 'Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-Mail within the prohibition of [the Wiretap Act] is virtually impossible.'

Even if the narrowest interpretation of "interception" was properly used by the MC (which plaintiff believes it *was not*) the MC's ruling remains flawed if only because of the type of acquisition evidenced in this case. In a somewhat similar case, *Blumofe v. Pharmatrak, Inc*., 329 F.3d 9 (1st Cir. 2003), the court noted that the concept of a contemporaneity or real-time requirement, which evolved in other factual contexts, may not be apt to address issues involving the application of the Wiretap Act to electronic communications. *Id*. at * 21-22. The court also found that interception would be justified even under the contemporaneous standard of intercept when a program automatically duplicated part of the communication between an user and intended recipient, and sent the information to a third party. *Id.* Cases such as *Pharmatrak* still support this case even under the narrowest definition of intercept available. In this case, Tech's software, *Webwatcher*, acted much like a data logging program, but after the data was recorded, it then *also acted* as an automatic routing program since the user never had to do anything to send the acquired information to Awareness Tech's private servers thousands of miles away. So the program *itself* automatically sent the information.

> We then noted that Pharmatrak's program would qualify under the *Steiger* definition because it effectively was an automatic routing program. Id. Much like the data logging program there, the Procmail recipe file here acted as an automatic routing program. It analyzed all of the e-mails sent to Councilman's mail server in real time and copied the relevant ones while they were being delivered.
>
> – *US v. Councilman*, 373 F. 3d 197 (1st Circuit 2004)("*Councilman II*")

Thus, the acquisition of Plaintiff's data in this case mimics that found in *Pharmatrak* and the software used also automatically re-routed the acquired information. Therefore, the reasoning used by the Court in *Councilman* should be instructive to this Court as it surely will be to the appellate court in the coming appeal. Therefore, whether right or wrong about its acceptance of

the narrowest reading of the already destructively narrow contemporaneous standard, Plaintiff retains standing because, as the Court in *Councilman* stated, "[e]ven those courts that narrowly read 'interception' would find that Pharmatrak's acquisition was an interception." *Id.* at 215.

The illegality of Awareness Tech's business model and its dangerous software should be obvious by now to anyone. This Court should finally recognize that illegal interceptions most assuredly happened here under *anyone's* definition of "contemporaneous" or their interpretation of "interception."

B. The MC Erred By Ignoring The Type Of Acquisition Involved In This Case

This case involves the *continuous, ongoing surveillance* of the contents of the Plaintiffs' incoming and outgoing electronic communications. Consistent with *Berger,* this Court should find that this conduct constitutes an "intercept" under the Wiretap Act. Any other holding will authorize warrantless that does not satisfy the requirements of Berger, which will create serious constitutional concerns.

One of the foremost experts dealing with the Wiretap Act, Professor Orin Kerr has explained: In Berger, the Supreme Court applied the Fourth Amendment where surveillance was performed as "a series [of intrusions] or a continuous surveillance" and not "one limited intrusion." 388 U.S. at 57. As a result, any statute that permits "a series or a period of continuous surveillance" must include rigorous privacy protections or may be facially invalid under the Fourth Amendment. Id. at 56; *Sibron v. New York*, 392 U.S. 40, 59-60 (1968) (noting that *Berger* struck down a New York statute setting forth a procedure for issuing wiretap warrants, but failing to include necessary safeguards to satisfy Fourth and Fourteenth Amendment scrutiny).

Keeping in mind the relationship between *Berger* and the Wiretap Act, any ambiguity in the Wiretap Act's language should be construed consistently with Berger's Fourth Amendment requirements. As a leading treatise on criminal procedure notes: Given the Wiretap Act's close connection to Berger, the meaning of "intercept" should mirror the distinction drawn by the Supreme Court in Berger. Acquisition is an intercept when it is part of "a series or a continuous surveillance," such as ongoing prospective surveillance or its functional equivalent. Exact lines will be difficult to draw, but the essential question should be whether the means of monitoring is the functional equivalent of continuous surveillance or whether it is more like a one-time or otherwise limited access to communications. LaFave, 2 CRIM. PROC. § 4.6(b).10

When stored communications are accessed in a way that makes the access the functional equivalent of a wiretap, the surveillance should be regulated by the Wiretap Act, not the SCA. For example, if an agent lines up a string of [18 U.S.C. §] 2703(a) orders and serves one order per hour, I think that is the functional equivalent of a wiretap. It is reasonable to infer that this case involves the continuous, ongoing surveillance of the contents of the Plaintiffs' incoming and outgoing electronic communications. Consistent with Berger, this Court should find that this conduct constitutes an "intercept" under the Wiretap Act. Any other holding will authorize warrantless that does not satisfy the requirements of Berger, which will create serious constitutional concerns.

IV. The MC Erred by dismissing privacy claims in part due to its belief that married people always lose their reasonable expectations of privacy in their marriage.

A. The MC erred by using improper case law to support its flawed decision

Once again the MC has improperly used a case as a primary reason to deny Plaintiff's claims. The MC has done this throughout the five years the case has been in this forum in order to bolster its false conclusions and dismissals of this case, thus Plaintiff is not surprised–rather, he expects it by now. As only one example of its error in this RR which mimics half a dozen similarly improper cases used within its first RR, we need go no further than the Court's use of of *White v. White*, 344 N.J. Super. 211, 781 A.2d 85 (2001). The MC felt this case was somehow "illustrative" during her twelve pages of reasoning wherein she ruled Tech was entitled to judgment on Plaintiff's breach of privacy claims (Doc.# 225 at*20-32) The MC did speak about how that court held that a spouse's access to e-mail was not "without authorization" and privacy interest was not "reasonable" where family computer was in area of marital residence where the entire family had access to it. And yet, as is apparently the MC's custom in the past five years through almost all of its orders and reports, only half the story was told; another half truth by the MC in a sea of half truths used by that court in the five years this case has been in this forum – nothing new to see here. Yet a fair and proper exploration would have also mentioned this other significant part of that case; not explored or mentioned, however, was the fact that in that case, the retrieved the emails were stored in an AOL folder located right on on family computer hard drive, and the wife didn't have to use a password or even access her husband's email account to get them. Because they were easily accessible, the court found the husband didn't have a reasonable expectation of privacy to the emails, and they were admissible. In contrast, in this case all the stolen information came from a password protected account, and of course the instant messages could not have been retrieved from any hard drive storage or folder. That's quite a huge difference, and it is one a fair court would have mentioned. Strike that… a fair court would not have used *White* as part of its failed attempt to dismiss this action, as *White* can be seen to

supports this case rather than defeat it. Sadly for the MC (not to mention this long suffering plaintiff), this is but one *of a dozen similar half truths* within the RR that this District Court should carefully consider before accepting that terribly flawed RR that will easily be defeated in appeals.[10] Thus, it would be easier for this to end right here rather than causing Plaintiff to go to the appellate court with a better case than he had in the first appeal when his complaint admittedly did leave much to be desired.

Regardless of those obvious errors, there are plenty of cases supporting the claim that spouses do not lose their fourth amendment rights when they get married. A person has an expectation of privacy when they are using a password protect ted account on ANYONE's computer - even God's if God resides within the US and one were to use his computer. One of

[10] For example, the MC's use of *Evans v. Evans*, 169 N.C.App. 358, 610 S.E.2d 264 (2005) is similarly improper as the e-mails in question were stored on and recovered from hard drive of family computer– which is whole different animal than what we have here where 95% of the acquired information came from RAM which is neither easily accessible as the information was in *Evans*. Yet the MC used it in support of denial of claims. And yet another perplexing use was on the same page, when the MC used *Bailey v. Bailey,* 2008 WL 324156 (E.D. Mich. Feb. 6, 2008) which seems to have been meant for another section of the RR where it could have been more properly (although ineffectively since it is hardly the same thing to retrieve mail form a password than what we have here) used as an example of a court denying ECPA claims due to lack of the contemporaneous requirement. All those obvious errors ON ONE PAGE! All throughout this case –plaintiff has suffered from what the press and likely Mueller is suffering now with this gangster presidency; i.e. so many scandals and problems, they don't know where to begin. In fact, the number of plain errors led the Vanderbilt clinic to forgo the initial thrust of my appeal, telling me that there were indeed so many errors, it would not allow them room for their primary ECPA issues. Plaintiff would exceed the page limit if he had to go into all of the similar errors found on the RR. They are simply too many, as they were in the MC's first three reports and recommendations and most of her orders. In fact, in both cases it might be by design, and so the analogy is likely more true than most can ever imagine. The many obvious errors leave Plaintiff quite confident as he heads towards appeals already with appeals lawyers requesting my approval to let them represent the case- no begging required this time. So apparent those errors n must be that I have received the requests without any inquiry – having believed the same clinic would again represent the case in the upcoming appeal. Obvious error will definitely be a central theme this time around, because once again the errors are far too many for any appeals court to expect a detailed objection of the many errors involved. .

those cases is *Lazette v. Kulmatycki*, where a former Verizon employee (Lazette) brought suit against her former employer and supervisor for, among other claims, violations of the Stored Communications Act (SCA) and invasion of privacy (a common law cause of action). Lazette alleged that her former supervisor read more than 48,000 of her personal email messages using the corporate-owned BlackBerry device she had recently turned back in to the company for recycling purposes. In response, Verizon and the former supervisor filed a motion to dismiss, claiming the SCA only applied to computer hackers. The court ruled that the defendants' interpretation of the Act was inaccurate. The court, referencing *Garcia v. City of Laredo, Tex*.[2], a Fifth Circuit Court of Appeals decision, emphasized the email account—not the device itself—was subject to the Act. Same applies here.

B. The area from which the information was taken is a fictitious legal construct provided by the Supreme Court interpretations of the Fourth Amendment and belonged only to Plaintiff and Catherine Zang – no-matter whose computer was used.

The Wiretap Act contains three different "Titles." Only the first two, Title I and Title II, are of relevance in this appeal. Generally speaking, Title I is implicated with the use of the spyware used in this case, and Title II is implicated when one hacks into another's email account. More specifically, Title II created the SCA to cover access to stored communications and records, and generally prohibits access to stored information on a server or computer. Unlike Title I,[11] the SCA applies only to stored communications. *See* 18 U.S.C. §2701(a); *Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 874 (9th Cir. 2002). Of primary concern in this appeal, the SCA creates criminal

[11] The terms "Title I", Wiretap Act," and "ECPA" are often used interchangeably in the legal arena. The ECPA was an amendment to Title III of the Omnibus Crime Control And Safe Streets Act ('OCCSSA'). Further confusing matters, OCCSSA itself is also known as "the Wiretap Statute." For the sake of clarity within this section, Title I will only apply to

and civil penalties against whoever "intentionally accesses without authorization a facility through which an electronic communication service is provided." 18 U.S.C. §§2701(a)(1). "Electronic communication service" is defined as "any service which provides users thereof the ability to send or receive wire or electronic communications." 18 U.S.C.§ 2510(15). Any company or government entity that provides others with the means to communicate electronically can be a "provider of electronic communication service" relating to the communications it provides, regardless of the entity's primary business or function. *See Fraser v. Nationwide Mut. Ins. Co. , 352* F.3d 107, 114-15 (3d Cir. 2004) (insurance company that provided email service to employees is an ECS). Appellee can be seen as providing its users the ability to send or receive electronic communications both to its servers, and from its servers to whatever computer or device they send or retrieve the stored messages.

Significantly, the SCA it is not limited to unlawful access to a computer or facility alone. Instead it also prohibits such access to a *network* without authorization. Therein lies a mildly complicated concept relevant to Appellant's SCA claims. At the time of the alleged violations of the Act by Tech, Appellant used various Internet Service Providers ('ISPs'), such as America Online ('AOL"), Yahoo, and Gmail to both send and receive emails and instant messages. All of the above ISPs are considered ECS as defined in the SCA. The majority of the relevant communications rerouted by Web Watcher onto Tech' private servers were obtained somewhere within a temporary amalgam of purpose created within cyberspace. This practically indefinable union of personal devices and infrastructure represented a communications tunnel or perhaps cubicle—practically a high tech virtual phone booth—carrying and temporarily hosting constitutionally protected communications. The tunnel is formed by a technically complex interaction between 1) Appellant's personal computer, 2) the privately owned servers and software

of AOL,[12] 3) the Internet's publically accessible infrastructure, and 4) the computer of the intended recipient of Appellant's communications, Ms Zang, who Appellant believes also primarily depended on those three ISP's for her Internet-based electronic communications. In addition to intercepting every single message both to and from Ms. Zang's computer, Web Watcher also recorded all of her browsing history and took snapshots of websites visited, as well as snapshots of instant message sessions, along with the intercept of those messages themselves. Obviously Web Watcher violated all aspects of the Wiretap Act concerning Ms. Zang. The question remains, what aspect did it violate against Appellant in this case? Firstly, a large volume of Instant message and emails originating from her computer in Ohio were inevitably re-routed onto Tech' own servers, summarized ('used') and delivered by Tech prior to Appellant having either received, or read those emails. Depending on the standards applied to such interceptions during a court's interpretation of the Act, those intercepts represent either a violation of the Act, or the SCA. Due to the way that the Internet works, and how information packets travel to and from many different servers, instead of directly to their intended recipients, courts applying the narrow interpretation of "intercept" have often ruled that such communications were not intercepted, but merely retrieved from temporary storage. In fact, for decades, small time hackers as well as larger entities of intercept–both public and private–have successfully depended on such a narrow interpretation by the judiciary in order to relieve themselves of liability under the Act. As far as Appellant knows, as he was effectively denied Discovery against Tech, Web Watcher was only installed on the Ohio computer.[13] The statute defines "intercept" as: "any temporary, immediate storage of wire or

[12] For the sake of simplicity, Appellant will use "AOL" to represent all of those ISPs during the rest of this discussion, for both his own use and Ms. Zang's. While this speaks of the SCA it also relevant for the Act itself.

[13] Appellant cannot know for certain, as Tech once sold a product that would automatically and surreptitiously install itself on the computer of a recipient who opened an otherwise innocent looking file, such as a picture sent from Ms. Zang. While Tech supposedly stopped selling that program prior to 2009, such information was not accessible to him in the lower proceedings.

electronic communications incidental to the electronic transmission thereof." The communications originating from Appellant's home in Florida were first sent to AOL, where they resided in temporary storage before AOL created a virtual tunnel within the Internet itself, wherein Appellants AOL account is temporarily "consolidated" with Ms. Zang's AOL account, opening a gateway between the two computers wherein the packets of information travelled on their way to and from Ohio. Prior to the communication reaching Ms. Zang's computer, where they would then be placed into temporary storage in some manner; likely the RAM.[14] Web Watcher then copied the information in a blink of an eye and either sent it immediately or funneled it onto her hard drive until the communication was over, wherein tech claims WebWatcher then transmitted a copy of the communications to Tech' personal servers, apparently somewhere in California. Thus the intercept or illegal access to the privileged communications did not physically occur on Appellant's computer, nor did they need to have been so accessed. Web Watcher may not have resided on his own computer hard drive, yet when Appellant sent communications towards the infected computer, it was surely accessing his communications somewhere within the tunnel created between his computer, AOL,[15] the Internet, and Ms. Zang's computer. That ineffable tunnel is rightly seen as an extension of all four of the entities involved. And yet in truth, there were five entities in that tunnel. However, one of those entities is not like the other. The uninvited outlier in this instance was, of course, Tech Technologies, whose advanced software, Web

[14] Although during its early years, AOL was used primarily from the desktop, and was not Internet based, the service began to mimic GMAIL and other such ISPs, in order to compete with those providers. Title II does not protect communications on a person's hard drive. Emails sent or received on AOL would typically be stored as a file on AOL's servers both prior and after their access by Appellant, or Ms. Zang—although in the case of a desktop client, they could be automatically saved on the hard drive, or of course downloaded from there to the hard drive. but such a practice is rare as they remain better protected on the ISP's servers. In the case of instant messages, the communications were placed within AOL's shared cache on her hard drive. Nonetheless, as stated above, Web Watcher intercepted and re-routed the communications prior to their placement on the hard drive, when they remained in "electronic storage."

[15] Because AOL is fully considered an ECS under the Act, improper access by Tech' mechanism of intercept, which effectively reached into the tunnel created by AOL is relevant to Appellant's SCA claims.

Watcher, operated as a kind of long armed "spike Mike;" an agent and extension of that company during the entire period of illegal intercepts. In effect, Web Watcher can be seen as having improperly accessed and obtained Appellants stored communications travelling within an extension of an ECS in violation of the SCA. Of course the same is applicable to messages being sent to Appellant.

Programs like Web Watcher that are designed to forward copies of incoming and outgoing messages, have sometimes been ruled to have violated Title I because they effectively intercept messages contemporaneously with transmission, or so close to being contemporaneous, that the distinction has recently begun to be ignored by many courts as being irrelevant—as it was in this case back in 2013 when this Court seemed to support the more advanced standards evidenced even in Circuits that do follow the "contemporaneous" standard of intercept. Support for Appellant's SCA claims can be found in various notable cases that have been faced with the task of determining whether obtaining another's email while that email is in "transient electronic storage" during the moments of transmission constitutes an "interception" under the Wiretap Act, as opposed to merely accessing data from "storage." *See eg. United States v. Councilman*, 418 F.3d 67, 83 (1st Cir. 2005)(en banc). *Councilman* focused on the determination of whether obtaining another's email while that email is in "transient electronic storage" during the moments of transmission constitutes an "interception" under the Wiretap Act, as opposed to merely accessing data from "storage." That temporary link, or tunnel, forms an extension of Appellant's own computer during the temporary interval where his computer has reached out into cyberspace. That otherwise ethereal amalgam of hardware and Internet infrastructure receives the same protection as the hard drive in Appellant's own computer, as Appellant's expectations of privacy extend into that immutable link, temporary or not. Thus the communications in temporary storage in cyberspace

that are intercepted and re-routed by Web Watcher are seen as effectively having been accessed from his computer hard drive. To further clarify, emails emanating from Appellant's own computer in Florida to Ohio were at some point in the transmission, accessed from RAM, copied and then re-routed by Web Watcher. That information, according to the narrow interpretation of intercept, happened while the electronic packets were in temporary *storage*, prior to the intended recipient having opened or read them– at least in some or even many cases. For example, Plaintiff could have been away from his computer while emails were received on his computer, but already copied by WebWatcher form Cathy's RAM. Same goes for instant messages. This Court presupposes that both sender and recipient are at their computers 24/7 monitoring each transmission live, which is an impractical fallacy. In fact a court in this circuit ruled Stored communications are covered by the SCA.[16]Therefore, even if this Court now chooses to reject the lower court's adoption of the re-routing standard of intercept during its exploration of intercept in its report, (XXX) and instead sticks with the narrow standard of intercept, Appellant's protected communications were in the least improperly accessed prior to their reach of Appellant's intended destination, and within a constitutionally protected sphere representing an extension of his own computer's hard drive, and so Tech' acquisition of same violated the provisions of the SCA.

Conclusion

At a critical time in our history, with a dangerous fascist administration led by a corrupt businessman seemingly hell-bent on ushering in the dystopian "corporatocracy" future of all our

[16] While the lower court rejected the contemporaneous standard of intercept, and so Appellant cannot have his cake and eat it too, that standard is, after all, the more narrow interpretation. By definition, the broader interpretation adopted by the lower court encompasses and exceeds that more narrow standard.

cumulative nightmares, history will prove that this is the wrong direction for us to take at the wrong time with the wrong topic. Online surveillance is rife and it is likely one of the most important issues facing our world. Yet, given all of the above, this Court has ruled that a company that advertises its surveillance technology for illegal intercept of information is basically untouchable by the justice system. Representing the absolute worst case scenario, the MC's ruling helps open the floodgates to corporate and private intercept at a scale no one here has ever imagined. If an intercept did not occur in this case, then the entire ECPA is a waste of time and energy and provides no realistic protection of our digital information at all!

This Court should take heed to the warnings of the very Court most responsible for causing this decades old privacy disaster. The Court in *Steiger* even went as far as to say, "Indeed, under the narrow reading of the Wiretap Act we adopt from the Fifth and Ninth Circuits, very few seizures of electronic communications from computers will constitute "'interceptions.'" This Court need not add its name to a long list of courts that will someday soon find themselves on the wrong side of history- and at the wrong moment in time.

I, Javier Luis hereby declare under penalty of perjury that the above is true and correct to the best of my knowledge and belief. I further certify that I am willing to testify under oath as to any and all claims.

/s/ Javier Luis

Dated: May 7, 2018

Respectfully Submitted,

/s/ Javier Luis
JDLuis65Ohio@gmail.com

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing Motion was filed electronically on May 7, 2018. Parties may access this document through that system.

/s/ Javier Luis, Pro Se